Configurar endpoints de serviços de plataforma

StorageGRID

NetApp
March 12, 2025

Índice

Configurar endpoints de serviços de plataforma

Antes de configurar um serviço de plataforma para um bucket, você deve configurar pelo menos um endpoint para ser o destino do serviço de plataforma.

O acesso a serviços de plataforma é ativado por locatário por administrador do StorageGRID. Para criar ou usar um endpoint de serviços de plataforma, você deve ser um usuário de locatário com permissão Gerenciar endpoints ou acesso raiz, em uma grade cuja rede foi configurada para permitir que os nós de storage acessem recursos de endpoint externos. Para um único locatário, você pode configurar um máximo de 500 endpoints de serviços de plataforma. Contacte o administrador do StorageGRID para obter mais informações.

O que é um endpoint de serviços de plataforma?

Ao criar um endpoint de serviços de plataforma, você especifica as informações que o StorageGRID precisa para acessar o destino externo.

Por exemplo, se você quiser replicar objetos de um bucket do StorageGRID para um bucket do Amazon S3, crie um endpoint de serviços de plataforma que inclua as informações e credenciais que o StorageGRID precisa para acessar o bucket de destino na Amazon.

Cada tipo de serviço de plataforma requer seu próprio endpoint, então você deve configurar pelo menos um endpoint para cada serviço de plataforma que você planeja usar. Depois de definir um endpoint de serviços de plataforma, você usa o URN do endpoint como o destino no XML de configuração usado para ativar o serviço.

Você pode usar o mesmo ponto de extremidade que o destino para mais de um intervalo de origem. Por exemplo, você pode configurar vários buckets de origem para enviar metadados de objetos para o mesmo endpoint de integração de pesquisa para que você possa realizar pesquisas em vários buckets. Você também pode configurar um bucket de origem para usar mais de um endpoint como destino, o que permite que você faça coisas como enviar notificações sobre a criação de objetos para um tópico do Amazon Simple Notification Service (Amazon SNS) e notificações sobre a exclusão de objetos para um segundo tópico do Amazon SNS.

Endpoints para replicação do CloudMirror

O StorageGRID é compatível com pontos de extremidade de replicação que representam buckets do S3. Esses buckets podem estar hospedados no Amazon Web Services, na mesma ou em uma implantação remota do StorageGRID ou em outro serviço.

Endpoints para notificações

O StorageGRID suporta endpoints Amazon SNS e Kafka. Os endpoints do Simple Queue Service (SQS) ou do AWS Lambda não são suportados.

Para endpoints Kafka, TLS mútuo não é suportado. Como resultado, se você tiver `ssl.client.auth` definido como `required` na configuração do seu broker Kafka, isso pode causar problemas de configuração do endpoint do Kafka.

Endpoints para o serviço de integração de pesquisa

O StorageGRID é compatível com endpoints de integração de pesquisa que representam clusters do Elasticsearch. Esses clusters do Elasticsearch podem estar em um data center local ou hospedados em uma nuvem da AWS ou em outro lugar.

O endpoint de integração de pesquisa refere-se a um índice e tipo específicos do Elasticsearch. Você deve criar o índice no Elasticsearch antes de criar o endpoint no StorageGRID, ou a criação do endpoint falhará. Você não precisa criar o tipo antes de criar o endpoint. O StorageGRID criará o tipo, se necessário, quando envia metadados de objeto para o endpoint.

Informações relacionadas

"Administrar o StorageGRID"

Especifique URN para endpoint de serviços de plataforma

Ao criar um endpoint de serviços de plataforma, você deve especificar um Nome de recurso exclusivo (URN). Você usará a URN para referenciar o endpoint quando criar um XML de configuração para o serviço da plataforma. A URNA para cada endpoint deve ser única.

O StorageGRID valida endpoints de serviços de plataforma à medida que os cria. Antes de criar um endpoint de serviços de plataforma, confirme se o recurso especificado no endpoint existe e se ele pode ser alcançado.

URNA elementos

A URNA para um endpoint de serviços de plataforma deve começar com `arn:aws` ou `urn:mysite`, da seguinte forma:

- Se o serviço estiver hospedado na Amazon Web Services (AWS), use `arn:aws`
- Se o serviço estiver hospedado no Google Cloud Platform (GCP), use `arn:aws`
- Se o serviço estiver hospedado localmente, use `urn:mysite`

Por exemplo, se você estiver especificando a URNA para um endpoint do CloudMirror hospedado no StorageGRID, a URNA pode começar com `urn:sgws`.

O próximo elemento da URNA especifica o tipo de serviço de plataforma, como segue:

Serviço	Tipo
Replicação do CloudMirror	`s3`
Notificações	`sns` ou `kafka`
Integração de pesquisa	`es`

Por exemplo, para continuar especificando a URN para um endpoint do CloudMirror hospedado no StorageGRID, você adicionaria `s3` ao GET `urn:sgws:s3`.

O elemento final da URNA identifica o recurso alvo específico no URI de destino.

Serviço	Recurso específico
Replicação do CloudMirror	`bucket-name`

Serviço	Recurso específico
Notificações	`sns-topic-name` ou `kafka-topic-name`
Integração de pesquisa	`domain-name/index-name/type-name` **Observação:** se o cluster Elasticsearch estiver configurado para criar índices automaticamente, você deverá criar o índice manualmente antes de criar o endpoint.

Urnas para serviços hospedados na AWS e no GCP

Para entidades da AWS e do GCP, a URN completa é um AWS ARN válido. Por exemplo:

- Replicação do CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notificações:

```
arn:aws:sns:region:account-id:topic-name
```

- Integração de pesquisa:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

> Para um endpoint de integração de pesquisa da AWS, o `domain-name` deve incluir a cadeia de carateres literal `domain/` , como mostrado aqui.

Urnas para serviços hospedados localmente

Ao usar serviços hospedados localmente em vez de serviços em nuvem, você pode especificar a URNA de qualquer forma que crie uma URNA válida e única, desde que a URNA inclua os elementos necessários na terceira e última posições. Você pode deixar os elementos indicados por opcional em branco, ou você pode especificá-los de qualquer forma que o ajude a identificar o recurso e tornar a URNA única. Por exemplo:

- Replicação do CloudMirror:

```
urn:mysite:s3:optional:optional:bucket-name
```

Para um endpoint do CloudMirror hospedado no StorageGRID, você pode especificar uma URNA válida que começa com `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notificações:

  Especifique um endpoint do Amazon Simple Notification Service:

  ```
  urn:mysite:sns:optional:optional:sns-topic-name
  ```

  Especifique um ponto final Kafka:

  ```
  urn:mysite:kafka:optional:optional:kafka-topic-name
  ```

- Integração de pesquisa:

  ```
  urn:mysite:es:optional:optional:domain-name/index-name/type-name
  ```

  > Para endpoints de integração de pesquisa hospedados localmente, o `domain-name` elemento pode ser qualquer string, desde que a URNA do endpoint seja única.

Criar endpoint de serviços de plataforma

Você deve criar pelo menos um endpoint do tipo correto antes de habilitar um serviço de plataforma.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Os serviços de plataforma foram ativados para sua conta de locatário por um administrador do StorageGRID.
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".
- O recurso referenciado pelo endpoint de serviços da plataforma foi criado:
  - Replicação do CloudMirror: Bucket do S3
  - Notificação de eventos: Tópico do Amazon Simple Notification Service (Amazon SNS) ou Kafka
  - Notificação de pesquisa: Índice Elasticsearch, se o cluster de destino não estiver configurado para criar índices automaticamente.
- Você tem as informações sobre o recurso de destino:
  - Host e porta para o URI (Uniform Resource Identifier)

  > Se você planeja usar um bucket hospedado em um sistema StorageGRID como endpoint para replicação do CloudMirror, entre em Contato com o administrador da grade para determinar os valores que você precisa inserir.

◦ Nome de recurso único (URN)

"Especifique URN para endpoint de serviços de plataforma"

◦ Credenciais de autenticação (se necessário):

Endpoints de integração de pesquisa

Para endpoints de integração de pesquisa, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- HTTP básico: Nome de usuário e senha

Endpoints de replicação do CloudMirror

Para replicação do CloudMirror, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta
- CAP (Portal de Acesso C2S): URL de credenciais temporárias, certificados de servidor e cliente, chaves de cliente e uma senha de chave privada do cliente opcional.

Endpoints do Amazon SNS

Para endpoints do Amazon SNS, você pode usar as seguintes credenciais:

- Chave de acesso: ID da chave de acesso e chave de acesso secreta

Pontos finais Kafka

Para endpoints do Kafka, você pode usar as seguintes credenciais:

- SASL/PLAIN: Nome de usuário e senha
- SASL/SCRAM-SHA-256: Nome de usuário e senha
- SASL/SCRAM-SHA-512: Nome de usuário e senha

◦ Certificado de segurança (se estiver usando um certificado de CA personalizado)

- Se os recursos de segurança do Elasticsearch estiverem ativados, você terá o privilégio de cluster do monitor para teste de conetividade e o privilégio de índice de gravação ou o Privileges de índice de índice e exclusão para atualizações de documentos.

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**. A página de endpoints dos serviços da plataforma é exibida.
2. Selecione **criar endpoint**.
3. Introduza um nome de apresentação para descrever brevemente o ponto final e a respetiva finalidade.

   O tipo de serviço de plataforma que o endpoint suporta é mostrado ao lado do nome do endpoint quando ele está listado na página Endpoints, para que você não precise incluir essas informações no nome.

4. No campo **URI**, especifique o URI (Unique Resource Identifier) do endpoint.

   Use um dos seguintes formatos:

```
https://host:port
http://host:port
```

Se você não especificar uma porta, as seguintes portas padrão serão usadas:

- Porta 443 para URIs HTTPS e porta 80 para URIs HTTP (a maioria dos endpoints)
- Porta 9092 para URIs HTTPS e HTTP (somente endpoints Kafka)

Por exemplo, o URI para um bucket hospedado no StorageGRID pode ser:

```
https://s3.example.com:10443
```

Neste exemplo, `s3.example.com` representa a entrada DNS para o IP virtual (VIP) do grupo StorageGRID high availability (HA) e `10443` representa a porta definida no ponto de extremidade do balanceador de carga.

> Sempre que possível, você deve se conectar a um grupo de HA de nós de balanceamento de carga para evitar um único ponto de falha.

Da mesma forma, o URI para um bucket hospedado na AWS pode ser:

```
https://s3-aws-region.amazonaws.com
```

> Se o endpoint for usado para o serviço de replicação do CloudMirror, não inclua o nome do bucket no URI. Você inclui o nome do bucket no campo **URN**.

5. Insira o Nome do recurso exclusivo (URN) para o endpoint.

> Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

6. Selecione **continuar**.
7. Selecione um valor para **tipo de autenticação**.

Endpoints de integração de pesquisa

Introduza ou carregue as credenciais para um endpoint de integração de pesquisa.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto
HTTP básico	Usa um nome de usuário e senha para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe

Endpoints de replicação do CloudMirror

Insira ou carregue as credenciais para um endpoint de replicação do CloudMirror.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto
CAP (Portal de Acesso C2S)	Usa certificados e chaves para autenticar conexões com o destino.	• URL de credenciais temporárias • Certificado CA do servidor (upload de arquivo PEM) • Certificado de cliente (upload de arquivo PEM) • Chave privada do cliente (upload de arquivo PEM, formato criptografado OpenSSL ou formato de chave privada não criptografado) • Senha de chave privada do cliente (opcional)

Endpoints do Amazon SNS

Insira ou carregue as credenciais de um endpoint do Amazon SNS.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
Chave de acesso	Usa credenciais de estilo AWS para autenticar conexões com o destino.	• ID da chave de acesso • Chave de acesso secreto

Pontos finais Kafka

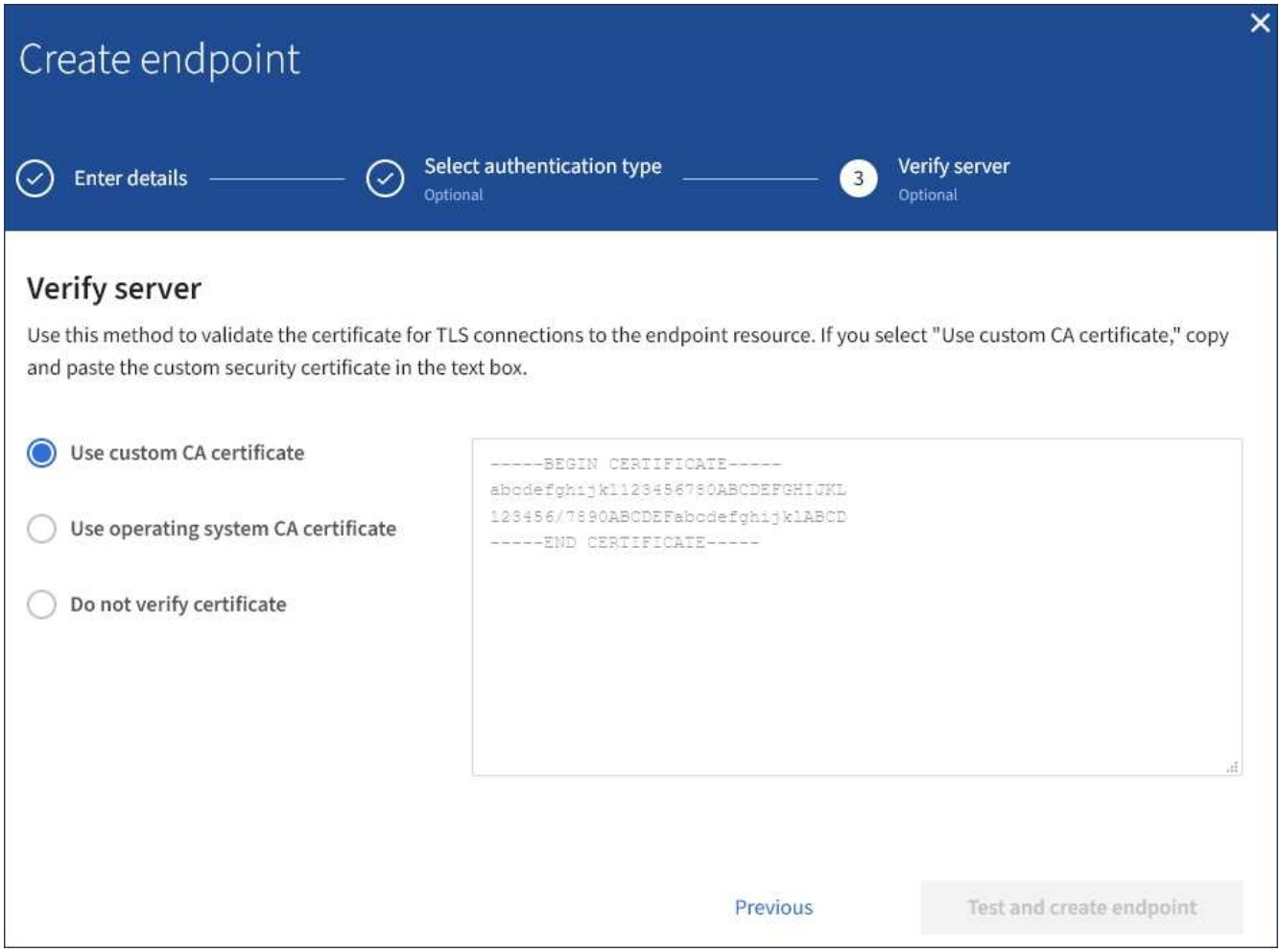
Introduza ou carregue as credenciais para um endpoint Kafka.

As credenciais fornecidas devem ter permissões de gravação para o recurso de destino.

Tipo de autenticação	Descrição	Credenciais
Anônimo	Fornece acesso anônimo ao destino. Funciona apenas para endpoints que têm a segurança desativada.	Sem autenticação.
SASL/PLANÍCIE	Usa um nome de usuário e senha com texto simples para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe
SASL/SCRAM-SHA-256	Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-256 para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe
SASL/SCRAM-SHA-512	Usa um nome de usuário e senha usando um protocolo de resposta a desafios e hash SHA-512 para autenticar conexões com o destino.	• Nome de utilizador • Palavra-passe

Selecione **usar autenticação de delegação tomada** se o nome de usuário e a senha forem derivados de um token de delegação obtido de um cluster Kafka.

8. Selecione **continuar**.
9. Selecione um botão de opção para **verificar servidor** para escolher como a conexão TLS com o endpoint é verificada.



Tipo de verificação do certificado	Descrição
Use certificado CA personalizado	Use um certificado de segurança personalizado. Se você selecionar essa configuração, copie e cole o certificado de segurança personalizado na caixa de texto **certificado CA**.
Use o certificado CA do sistema operacional	Use o certificado de CA de grade padrão instalado no sistema operacional para proteger conexões.
Não verifique o certificado	O certificado usado para a conexão TLS não é verificado. Esta opção não é segura.

10. Selecione **testar e criar endpoint**.
    - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
    - Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **retornar aos detalhes do endpoint** e atualize as informações. Em seguida, selecione **testar e criar endpoint**.

> A criação de endpoint falha se os serviços de plataforma não estiverem ativados para sua conta de locatário. Contacte o administrador do StorageGRID.

Depois de configurar um endpoint, você pode usar seu URN para configurar um serviço de plataforma.

Informações relacionadas

"Especifique URN para endpoint de serviços de plataforma"

"Configurar a replicação do CloudMirror"

"Configurar notificações de eventos"

"Configurar o serviço de integração de pesquisa"

Teste a conexão para endpoint de serviços de plataforma

Se a conexão com um serviço de plataforma tiver sido alterada, você pode testar a conexão para que o endpoint valide que o recurso de destino existe e que ele pode ser alcançado usando as credenciais especificadas.

Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

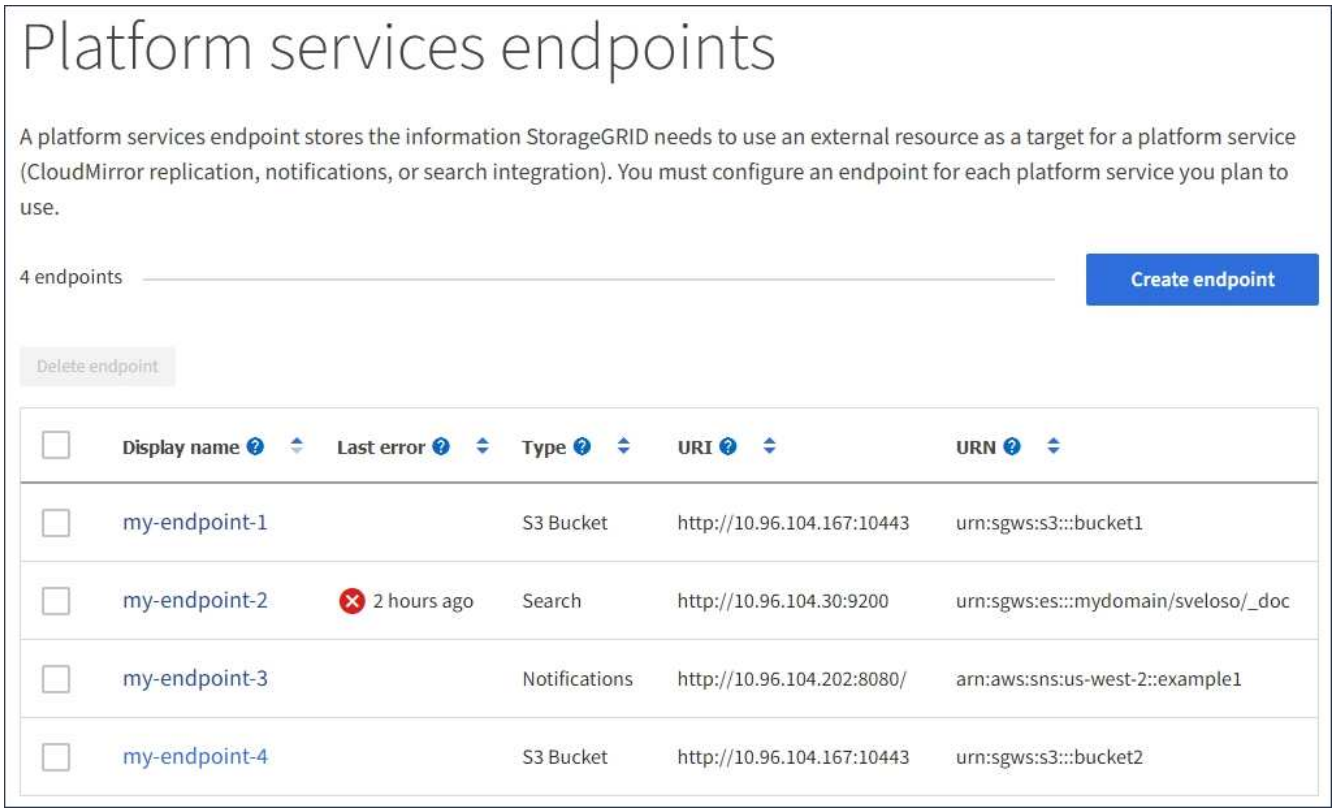
Sobre esta tarefa

O StorageGRID não valida se as credenciais têm as permissões corretas.

Passos

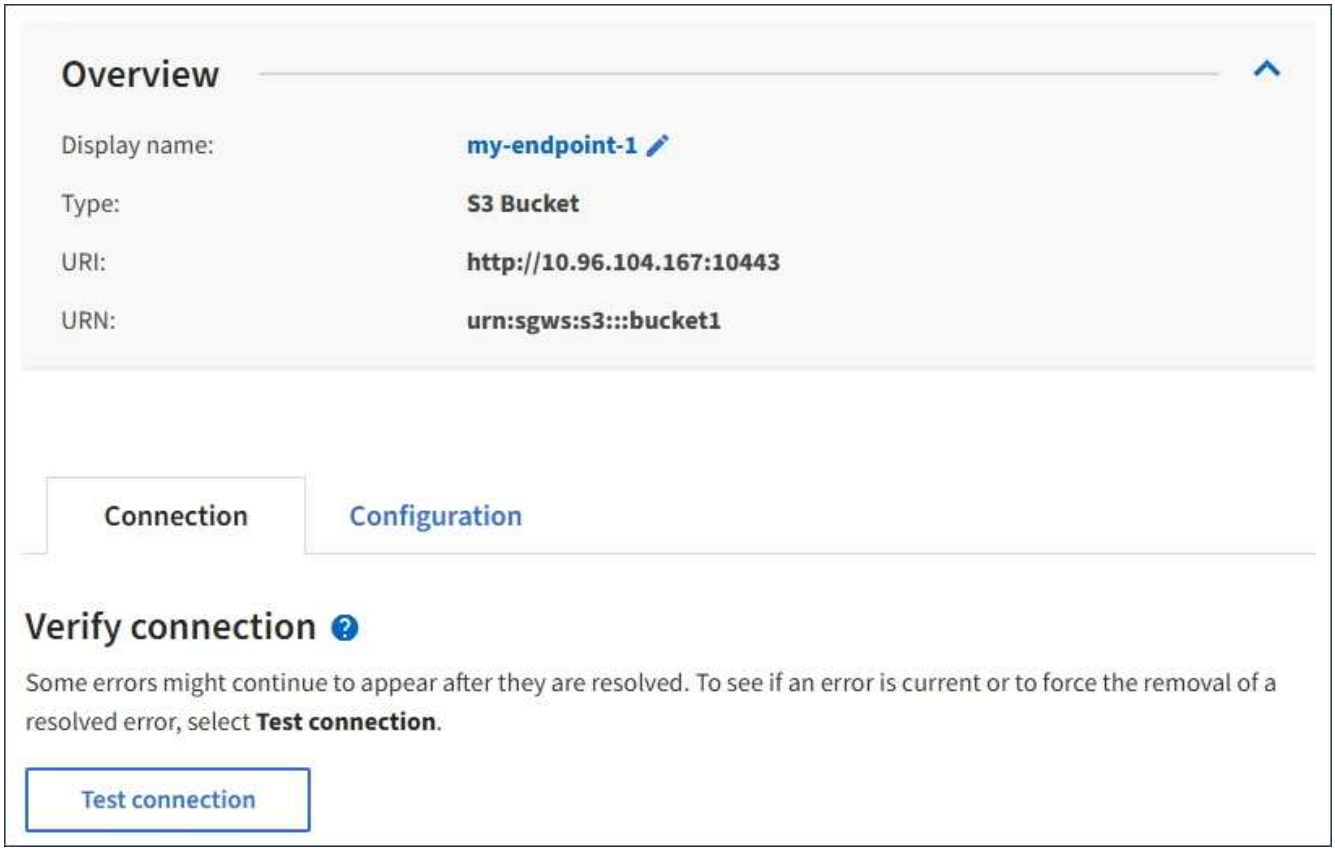
1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.



2. Selecione o ponto final cuja ligação pretende testar.

   A página de detalhes do ponto final é exibida.



3. Selecione **Test Connection**.

- Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é validada a partir de um nó em cada local.
- Uma mensagem de erro será exibida se a validação do endpoint falhar. Se você precisar modificar o endpoint para corrigir o erro, selecione **Configuração** e atualize as informações. Em seguida, selecione **testar e salvar alterações**.

Editar endpoint de serviços de plataforma

Você pode editar a configuração de um endpoint de serviços de plataforma para alterar seu nome, URI ou outros detalhes. Por exemplo, talvez seja necessário atualizar credenciais expiradas ou alterar o URI para apontar para um índice de backup do Elasticsearch para failover. Não é possível alterar a URN para um endpoint de serviços de plataforma.

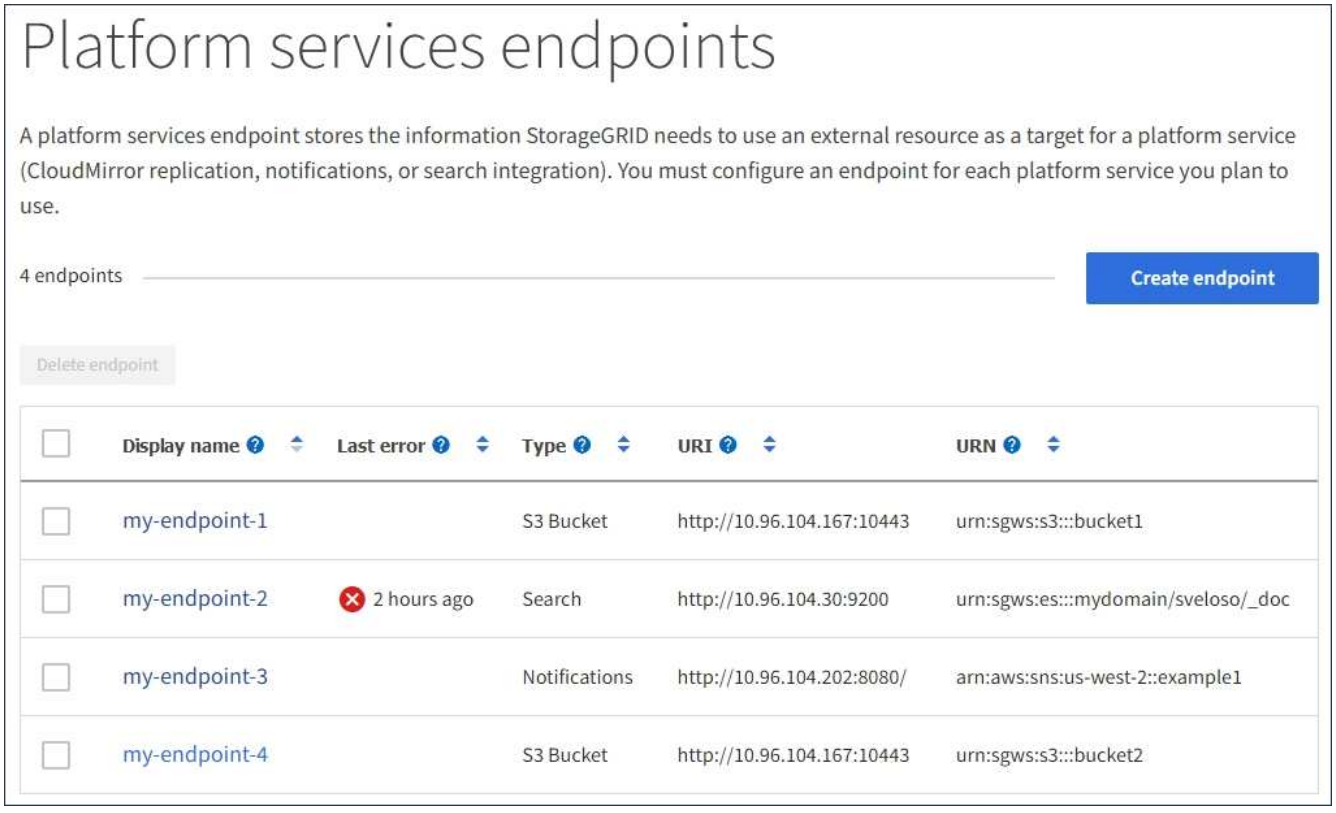
Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.



2. Selecione o ponto de extremidade que pretende editar.

   A página de detalhes do ponto final é exibida.

3. Selecione **Configuração**.
4. Conforme necessário, altere a configuração do endpoint.

   Você não pode alterar a URNA DE um endpoint depois que o endpoint foi criado.

   a. Para alterar o nome de exibição do endpoint, selecione o ícone de edição .
   b. Conforme necessário, altere o URI.
   c. Conforme necessário, altere o tipo de autenticação.
      - Para autenticação da chave de acesso, altere a chave conforme necessário selecionando **Editar chave S3** e colando uma nova ID de chave de acesso e chave de acesso secreta. Se você precisar cancelar suas alterações, selecione **Reverter S3 key edit**.
      - Para autenticação CAP (C2S Access Portal), altere a URL de credenciais temporárias ou a senha de chave privada do cliente opcional e carregue novos arquivos de certificado e chave conforme necessário.

        A chave privada do cliente deve estar no formato encriptado OpenSSL ou no formato de chave privada não encriptada.

   d. Conforme necessário, altere o método para verificar o servidor.
5. Selecione **Teste e salve as alterações**.
   - Uma mensagem de sucesso será exibida se o endpoint puder ser alcançado usando as credenciais especificadas. A conexão com o endpoint é verificada a partir de um nó em cada local.
   - Uma mensagem de erro será exibida se a validação do endpoint falhar. Modifique o ponto final para corrigir o erro e selecione **testar e salvar alterações**.

Excluir endpoint de serviços de plataforma

Você pode excluir um endpoint se não quiser mais usar o serviço de plataforma associado.

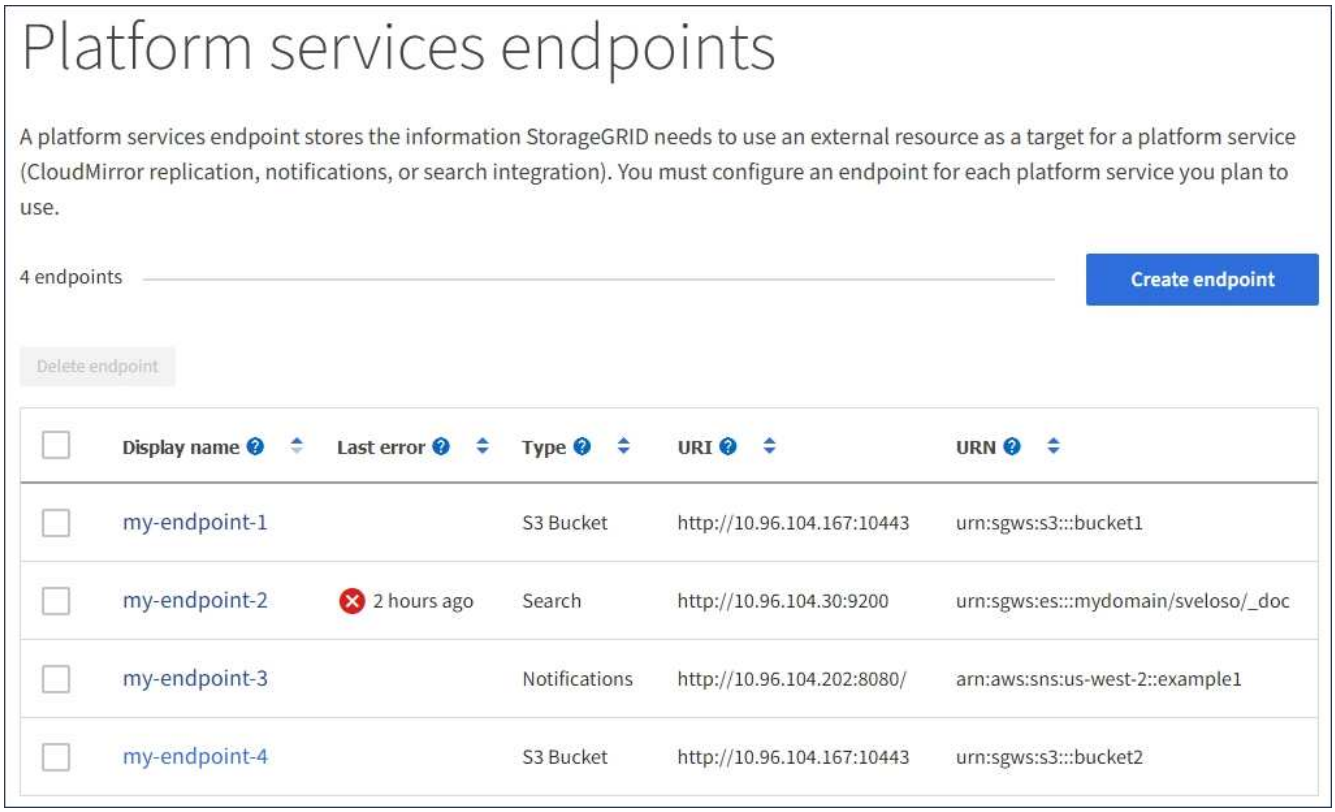
Antes de começar

- Você está conetado ao Gerenciador do Locatário usando um "navegador da web suportado".
- Você pertence a um grupo de usuários que tem o "Gerencie endpoints ou permissão de acesso root".

Passos

1. Selecione **STORAGE (S3)** > **endpoints de serviços de plataforma**.

   A página de endpoints de serviços da plataforma é exibida e mostra a lista de endpoints de serviços da plataforma que já foram configurados.

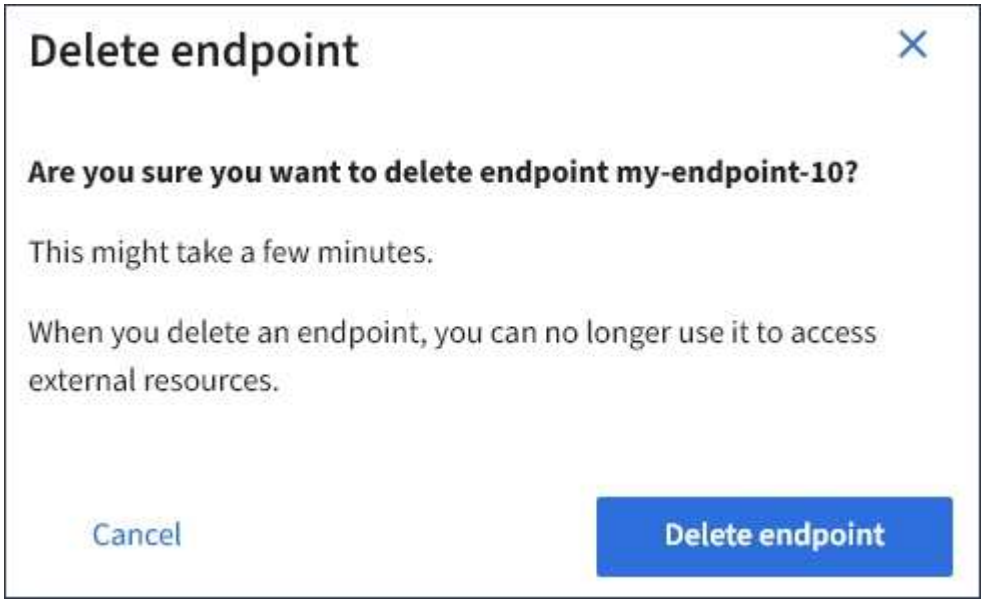


2. Selecione a caixa de verificação para cada ponto de extremidade que pretende eliminar.

> Se você excluir um endpoint de serviços de plataforma que está em uso, o serviço de plataforma associado será desativado para quaisquer buckets que usam o endpoint. Quaisquer solicitações que ainda não foram concluídas serão descartadas. Todas as novas solicitações continuarão sendo geradas até que você altere a configuração do bucket para não fazer mais referência à URNA excluída. O StorageGRID reportará essas solicitações como erros irrecuperáveis.

3. Selecione **ações** > **Excluir endpoint**.

   É apresentada uma mensagem de confirmação.



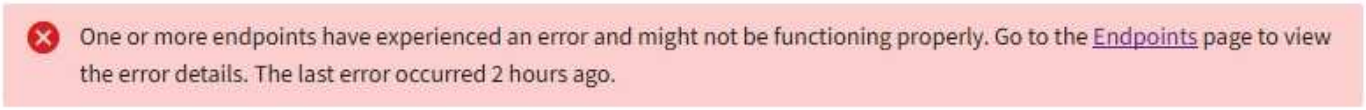
4. Selecione **Excluir endpoint**.

Solucionar erros de endpoint dos serviços da plataforma

Se ocorrer um erro quando o StorageGRID tenta se comunicar com um endpoint de serviços de plataforma, uma mensagem é exibida no painel. Na página pontos finais dos serviços da plataforma, a coluna último erro indica quanto tempo atrás o erro ocorreu. Nenhum erro é exibido se as permissões associadas às credenciais de um endpoint estiverem incorretas.

Determine se ocorreu um erro

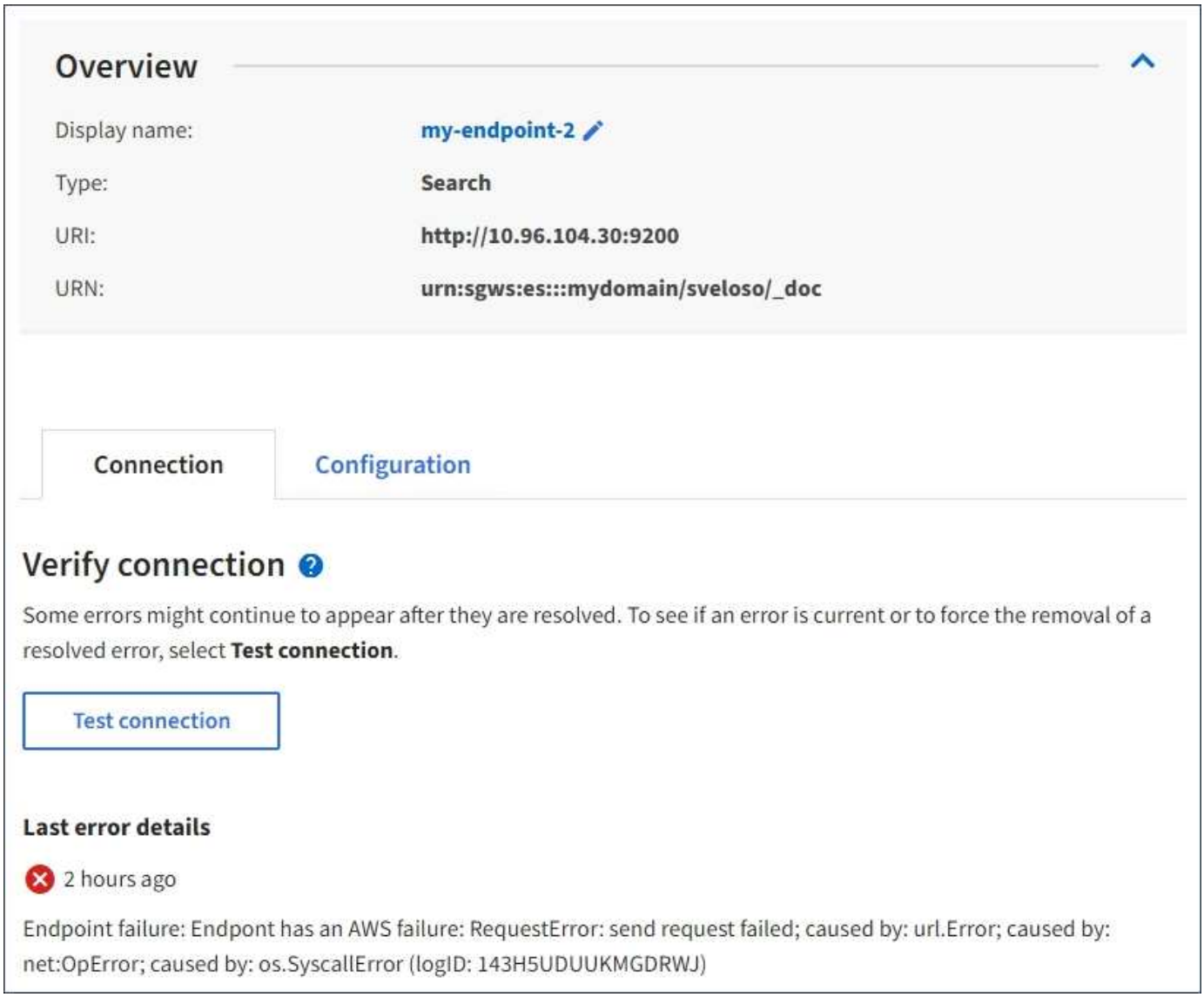
Se algum erro de endpoint de serviços de plataforma tiver ocorrido nos últimos 7 dias, o painel do Gerenciador do Locatário exibirá uma mensagem de alerta. Você pode acessar a página de endpoints dos serviços da plataforma para ver mais detalhes sobre o erro.



O mesmo erro que aparece no painel também aparece na parte superior da página de endpoints dos serviços da plataforma. Para ver uma mensagem de erro mais detalhada:

Passos

1. Na lista de endpoints, selecione o endpoint que tem o erro.
2. Na página de detalhes do endpoint, selecione **conexão**. Esta guia exibe apenas o erro mais recente para um endpoint e indica quanto tempo atrás o erro ocorreu. Erros que incluem o ícone X vermelho  ocorreram nos últimos 7 dias.



Verifique se o erro ainda está atual

Alguns erros podem continuar a ser mostrados na coluna **último erro** mesmo depois de resolvidos. Para ver se um erro é atual ou forçar a remoção de um erro resolvido da tabela:

Passos

1. Selecione o ponto final.

   A página de detalhes do ponto final é exibida.

2. Selecione **Connection** > **Test Connection**.

Selecionar **testar conexão** faz com que o StorageGRID valide que o endpoint dos serviços da plataforma existe e que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

Resolver erros de endpoint

Você pode usar a mensagem **último erro** na página de detalhes do endpoint para ajudar a determinar o que está causando o erro. Alguns erros podem exigir que você edite o endpoint para resolver o problema. Por

exemplo, um erro de espelhamento de nuvem pode ocorrer se o StorageGRID não conseguir acessar o bucket do destino S3 porque ele não tem as permissões de acesso corretas ou a chave de acesso expirou. A mensagem é "as credenciais de endpoint ou o acesso de destino precisa ser atualizado", e os detalhes são "AccessDenied" ou "InvalidAccessKeyId".

Se você precisar editar o endpoint para resolver um erro, selecionar **testar e salvar alterações** faz com que o StorageGRID valide o endpoint atualizado e confirme que ele pode ser alcançado com as credenciais atuais. A conexão com o endpoint é validada a partir de um nó em cada local.

Passos

1. Selecione o ponto final.
2. Na página de detalhes do endpoint, selecione **Configuração**.
3. Edite a configuração do endpoint conforme necessário.
4. Selecione **Connection** > **Test Connection**.

Credenciais de endpoint com permissões insuficientes

Quando o StorageGRID valida um endpoint de serviços de plataforma, ele confirma que as credenciais do endpoint podem ser usadas para entrar em Contato com o recurso de destino e faz uma verificação básica de permissões. No entanto, o StorageGRID não valida todas as permissões necessárias para determinadas operações de serviços de plataforma. Por esse motivo, se você receber um erro ao tentar usar um serviço de plataforma (como "403 proibido"), verifique as permissões associadas às credenciais do endpoint.

Informações relacionadas

- **Administrar o StorageGRID › solucionar problemas de serviços da plataforma**
- "Criar endpoint de serviços de plataforma"
- "Teste a conexão para endpoint de serviços de plataforma"
- "Editar endpoint de serviços de plataforma"

Informações sobre direitos autorais

Informações sobre marcas comerciais